WE CLAIM:

1. A method of encoding a common data stream for distribution to a plurality of destination systems, each destination system being authorized to access at least a portion of the common data stream, the method comprising:

obtaining a source stream;

identifying a first set of blocks of said source stream as secure blocks;

identifying a second set of blocks of said source stream as unsecure blocks;

encrypting said secure blocks for each of a plurality of classes of destination systems, thereby forming a plurality of encrypted secured block sets, such that an encrypted secured block set is decryptable by destination systems in a class associated with that encrypted secured block set; and

grouping said unsecured blocks and the plurality of encrypted secured block sets as the common data stream.

2. The method of claim 1, wherein said source stream is packetized video data.

3. The method of claim 1, further comprising encrypting unsecure blocks such that said unsecure blocks are decryptable by each of said plurality of destination systems, if authorized by at least one conditional access system.

4. The method of claim 1, wherein encrypting comprises encryption utilizing at least one of AES, with at least one AES key per class of destination systems, and DES, with at least one DES key per class of destination systems.

5. The method of claim 1, wherein said blocks are MPEG blocks and said secure blocks represent MPEG I frames.

6. A method of decoding a common data stream distributed to a plurality of destination systems, wherein said common data stream includes secure and unsecure blocks of

data, said secure blocks being encrypted for each of a plurality of classes of destination systems, respectively, said method comprising:

obtaining said common data stream;

decrypting said secure blocks for a native class of a destination system; and

grouping said unsecure blocks and said decrypted secure block sets as a useful stream for use by said destination system.

7. The method of claim 6 further comprising demultiplexing said common data stream into said secure and said unsecure blocks.

8. The method of claim 6, wherein decrypting comprises decryption utilizing at least one of AES, with at least one AES key per class of destination systems, , and DES, with at least one DES key per class of destination systems.

9. The method of claim 6 further comprising providing a decryption key for said step of decrypting.

10. The method of claim 6 further comprising discarding secure blocks of any non-native class.

11. The method of claim 6, wherein said blocks are MPEG blocks and said secure blocks represent MPEG I frames.

12. An encoder system for encoding a common data stream for distribution to a plurality of destination systems, each destination system being authorized to access at least a portion of the common data stream, said encoder system comprising:

an input for receiving a source stream;

an encoder, said encoder receiving said source stream and packetizing said source stream to provide a plurality of packets; and

an encryptor for selectively identifying at least one set of blocks of said packets as secure blocks and encrypting said secure blocks for each of a plurality of classes of destination systems, thereby forming a plurality of encrypted secured block sets, such that an

encrypted secured block set is decryptable by destination systems in a class associated with that encrypted secured block set.

13. The encoder system of claim 12, wherein said encryptor combines said encrypted secure blocks and said unsecure blocks to form a common data stream.

14. The encoder system of claim 12, wherein said encoder is an MPEG encoder.

15. The encoder system of claim 12, wherein said encyptor is at least one of a DES encyptor and an AES encyptor.

16. An encoder system for encoding a common data stream for distribution to a plurality of destination systems, each destination system being authorized to access at least a portion of the common data stream, said encoder system comprising:

an input for receiving a source stream;

an encoder, said encoder receiving said source stream and packetizing said source stream to provide a plurality of packets;

encryption selector for selectively identifying at least one set of blocks of said packets as secure blocks; and

an encryptor for encrypting said secure blocks for each of a plurality of classes of destination systems, thereby forming a plurality of encrypted secured block sets, such that an encrypted secured block set is decryptable by destination systems in a class associated with that encrypted secured block set.

17. The encoder system of claim 16, wherein said encryptor combines said encrypted secure blocks and said unsecure blocks to form a common data stream.

18. The encoder system of claim 16, wherein said encoder is an MPEG encoder.

19. The encoder system of claim 16, wherein said encyptor is at least one of a DES encyptor and an AES encryptor.

20. A decoder for decoding a useful signal stream from a common stream coded for use by a plurality of classes of destination systems, the decoder comprising:

a packet input, for receiving packets of said common stream;

a packet-type detector, for detecting if a received packet is an unsecure packet or a secure packet, and for said secured packets, detecting if the secured packet is designated for a native destination system class;

a decryptor for decrypting secured packets that are said native destination system class; and

a reassembler for reassembling the useful signal stream from any of said unsecure packets and said secure packets decrypted by said decryptor.

21. The decoder of claim 20, further comprising a discarder for discarding secure packets that are not designated for a destination system class that includes the destination system of the decoder.

22. The decoder of claim 20, wherein said reassembler comprises a MPEG decoder.

23. The decoder of claim 20, wherein the decryptor is at least one of a DES decryptor, and an AES encryptor.

24. A content transport system, comprising:

a selector for selecting blocks to be encrypted as secured blocks;

a secure block multi-encryptor, for encrypting said secured blocks for each of a plurality of classes of destination systems, thereby forming a plurality of encrypted secured block sets, such that an encrypted secured block set is decryptable by destination systems in the class associated with that encrypted secure block set;

a combiner for combining unsecure blocks and secure blocks into a common stream;

a demultiplexer for separating said common stream into blocks that are usable by a destination system and blocks that are not usable by the destination system;

a selective decryptor that decrypts usable secured blocks; and

a reassembler for reassembling a useful signal stream from any unsecure blocks, and said secure blocks decrypted by the selective decryptor, wherein an ability to reassemble the useful signal stream relies in part on an ability to decrypt usable secure blocks.

25. The system of claim 24, wherein the reassembler is an MPEG decoder.

26. A computer-readable carrier including a common data stream comprising:

a plurality of secure blocks encoded from a source stream, said plurality of secure blocks encrypted for each of a plurality of classes of destination systems, thereby forming a plurality of encrypted secured block sets, such that an encrypted secured block set is decryptable by destination systems in a class associated with that encrypted secured block set; and

a plurality of unsecured blocks encoded from said source stream.

27. A computer-readable carrier including computer program instructions for distribution to a plurality of destination systems, each destination system being authorized to access at least a portion of the common data stream that instruct a computer to perform the steps of:

obtaining a source stream;

identifying a first set of blocks of said source stream as secure blocks;

identifying a second set of blocks of said source stream as unsecure blocks;

encrypting said secure blocks for each of a plurality of classes of destination systems, thereby forming a plurality of encrypted secured block sets, such that an encrypted secured block set is decryptable by destination systems in a class associated with that encrypted secured block set; and

grouping said unsecured blocks and the plurality of encrypted secured block sets as the common data stream.

28. A computer-readable carrier including computer program instructions for decoding a common data stream distributed to a plurality of destination systems, wherein said common data stream includes secure and unsecure blocks of data, said secure blocks being encrypted for each of a plurality of classes of destination systems, respectively, that instruct a computer to perform the steps of:

obtaining said common data stream;

decrypting said secure blocks for a native class of a destination system; and

grouping said unsecure blocks and said decrypted secure block sets as a useful stream for use by said destination system.